Exhibit A
(Search Warrant)

UNITED STATES DISTRICT COURT

for the

District of Nevada

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The business and Federal Firearms Licensee ("FFL") known as POLYMER80, Inc. ("POLYMER80"), which is located at 134 Lakes Blvd, Dayton, NV 89403	)	Case No. **3:20-mj-123-WGC**

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Nevada
(identify the person or describe the property to be searched and give its location):

The business and Federal Firearms Licensee ("FFL") known as POLYMER80, Inc. ("POLYMER80"), which is located at 134 Lakes Blvd, Dayton, NV 89403, as further described in Attachment A, attached hereto and incorporated herein by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before 23 Dec 2020 *(not to exceed 14 days)*

☒ between the hours of 5:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to WILLIAM G. COBB .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 8 December 2020 11:15 a.m.

William G. Cobb
Judge's signature

City and state: Reno, Nevada

WILLIAM G. COBB, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

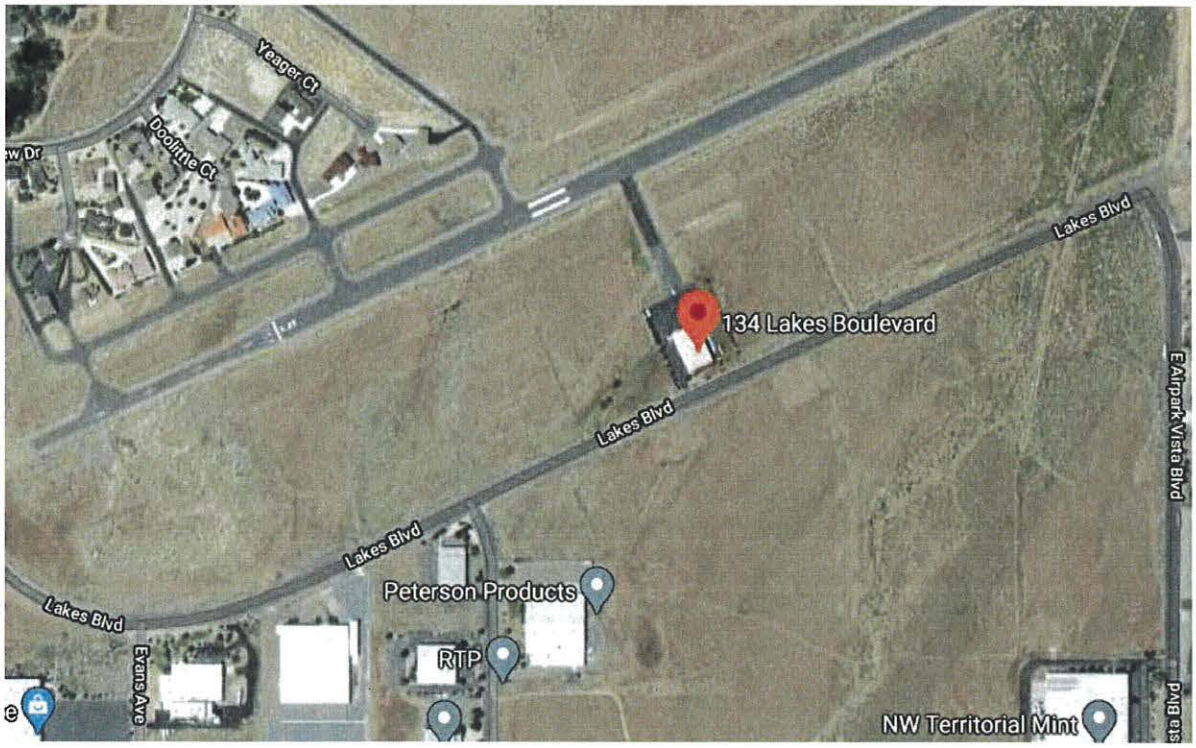
PREMISES TO BE SEARCHED

The business and Federal Firearms Licensee ("FFL") known as POLYMER80, Inc. ("POLYMER80"), which is located at 134 Lakes Blvd, Dayton, NV 89403 (the "SUBJECT PREMISES").

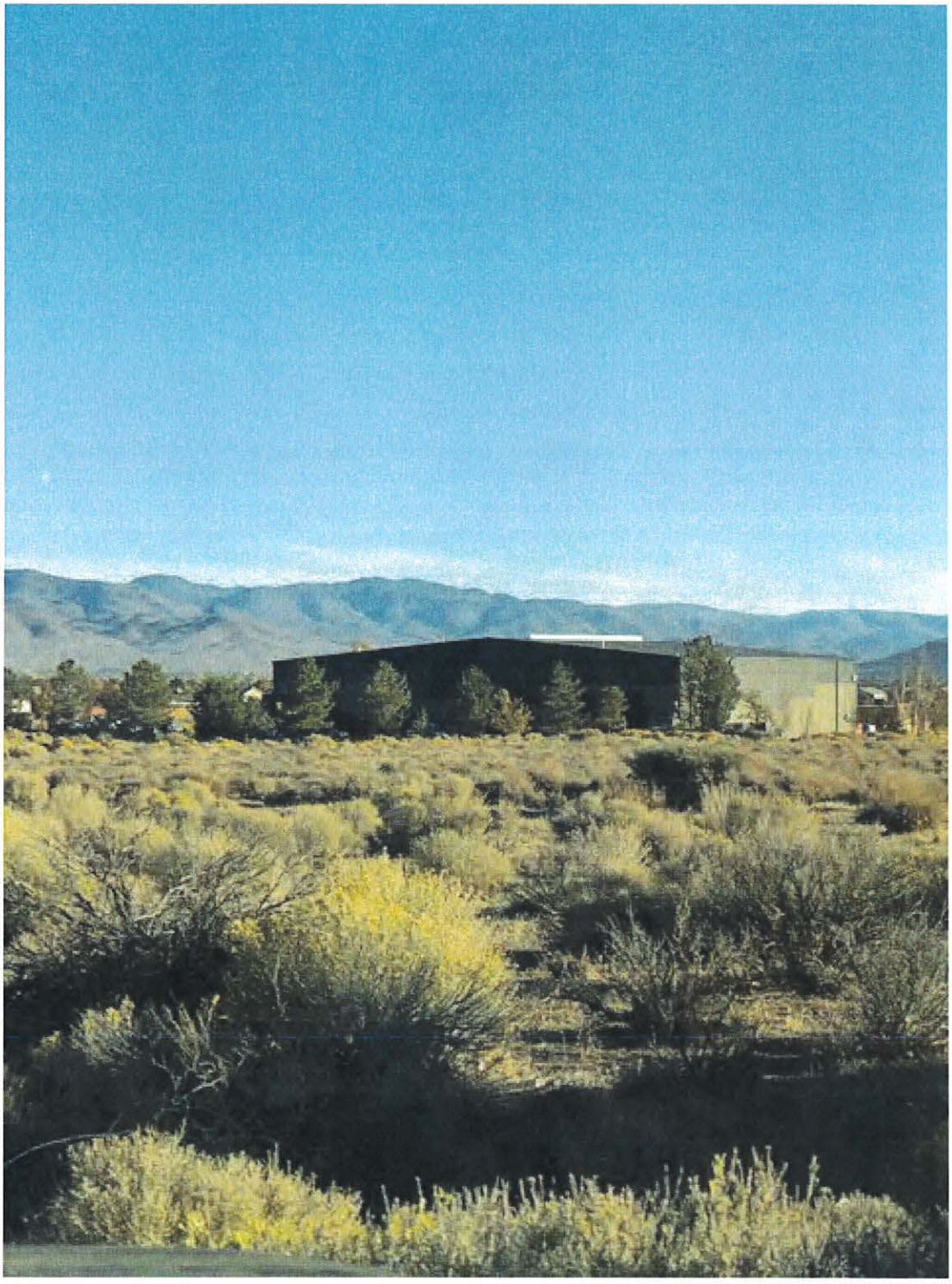
The SUBJECT PREMISES is a three acre plot of land containing a large single story tan and gray building, located on the northwest side of Lakes Blvd, and southeast of the Dayton Air Park airstrip.

The area to be searched at the SUBJECT PREMISES includes all rooms, trash containers, debris boxes, locked containers and safes, cabinets, garages, warehouses, or storage containers or other storage locations assigned to the SUBJECT PREMISES.

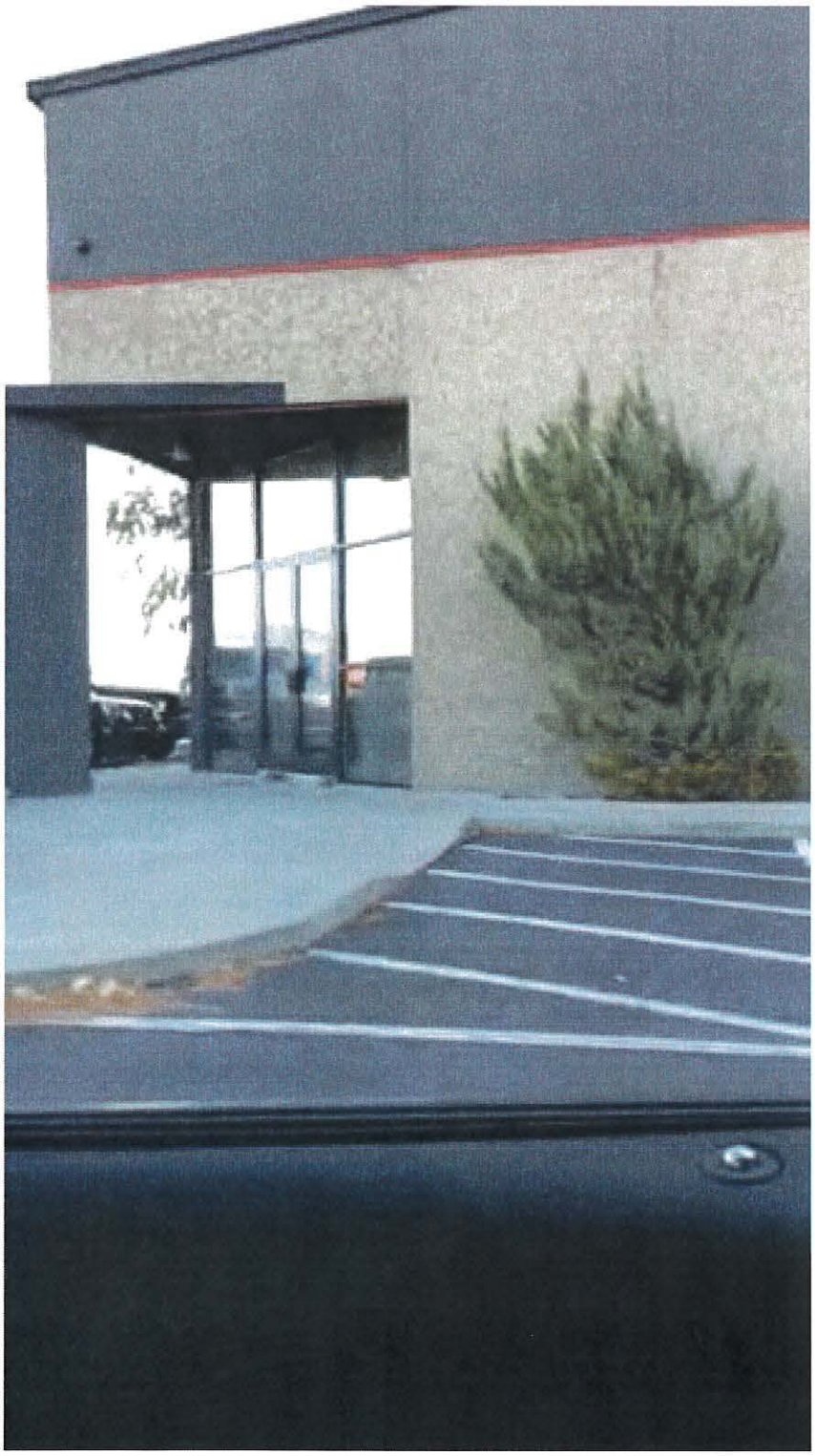
Overhead view of SUBJECT PREMISES



SUBJECT PREMISES



Main Entrance to SUBJECT PREMISES



ATTACHMENT B

I. ITEMS TO BE SEIZED:

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 922(a)(2) (Shipment or Transport of a Firearm by a Federal Firearms Licensee ("FFL") to a Non-FFL in Interstate or Foreign Commerce); 922(b)(2) (Sale or Delivery of a Firearm in Violation of State Law or Ordinance); 922(b)(3) (Sale or Delivery of a Firearm by an FFL to Person Not Residing in the FFL's State); 922(b)(5) (Sale or Delivery of a Firearm by an FFL Without Notating Required Information in Records); 922(d) (Sale or Disposition of a Firearm to a Prohibited Person); 922(e) (Delivery of a Package Containing a Firearm to a Common Carrier Without Written Notice); 922(g) (Possession of a Firearm by a Prohibited Person); 922(m) (False Records by an FFL); 922(t) (Knowing Transfer of Firearm without a Background Check); 922(z) (Sale, Delivery, or Transfer of a Handgun by an FFL Without a Secure Gun Storage or Safety Device); 371 (Conspiracy); and 22 U.S.C. §§ 2278(b)(2) and (c) and 50 U.S.C. § 4819 (Violations of the Arms Export Control Act and Export Control Regulations) (collectively, the "Subject Offenses"), namely:

a. "Buy, Build, Shoot" kits and components of "Buy, Build, Shoot" kits compiled or arranged in close proximity to one another indicating they were intended to be compiled into "Buy, Build, Shoot" kits;

b. Handguns bearing no serial number;

c. Communications and records concerning the manufacture, design, marketing, sale, shipment, and transfer of "Buy, Build, Shoot" kits;

d. Communications and records concerning federal, state, and local firearms laws and regulations;

e. Communications and records concerning "Buy Build Shoot" kits, or any other similar grouping of components that can be readily assembled into a firearm;

f. Communications and records of payments for and shipments of "Buy Build Shoot" kits or any other similar grouping of components that can be readily assembled into a firearm;

g. Communications and records concerning the sale or shipment of firearms and firearm components to individuals prohibited from possessing firearms;

h. Communications and records concerning the sale or shipment of firearms or firearm components to individuals or locations outside of the United States;

i. Records concerning the sale or transfer of firearms, including FFL Acquisition and Disposition records, ATF Form 4473s, NICS inquiries and background checks, and other records required to be maintained by FFLs;

j. Communications and records concerning the sale or transfer of firearms and firearm components to locations or individuals outside of the United States;

k. Information relating to the identity of the person(s) who communicated about matters discussed above;

l. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

m. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

4. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

5. Prior to reading any document or other piece of evidence ("document") in its entirety, law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search (the "Search Team") will conduct a limited review of the document in order to determine whether or not the document appears to contain or refer to communications between an attorney, or to contain the work product of an attorney, and any person ("potentially privileged information"). If a Search Team member determines that a document appears to contain potentially privileged information, the Search Team member will not continue to review the document and will immediately notify a member of the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case). The Search Team will not further review any document that appears to contain potentially privileged information until after the Privilege Review Team has completed its review.

6. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged

information to confirm that it contains potentially privileged information. If it does not, it may be returned to the Search Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

7. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Search Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Digital Evidence

8. The Search Team will search for digital devices capable of being used to facilitate the Subject Offenses or capable of containing data falling within the scope of the items to be seized. The Privilege Review Team will then review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

9. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

10. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

11. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like names of any identified attorneys or law firms or their email addresses, and generic words such as "privileged" or "work product". The Privilege Review Team will conduct an initial review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The

Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

12. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

13. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search

Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

14. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

15. Neither the Privilege Review Team nor the Search Team will seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

16. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

17. If the search determines that a digital device does contain data falling within the list of items to be seized, the

government may make and retain copies of such data, and may access such data at any time.

18. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

19. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

20. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

21. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the

custody and control of attorneys for the government and their support staff for their independent review.

22. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the Subject Offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

23. The special procedures relating to digital devices found in this warrant govern only the search of digital devices

pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.